OSteen MacLeod Combs

Lincoln Combs, State Bar No. 025080
**O'STEEN MACLEOD COMBS PLC**
300 W. Clarendon Ave., Suite 400
Phoenix, Arizona 85013-3424
T: (602) 252-888 F: (602)-274-1209
lcombs@omclawyers.com

Lynn A. Toops (*pro hac vice* forthcoming)
Amina A. Thomas (*pro hac vice* forthcoming)
**COHENMALAD, LLP**
One Indiana Square, Suite 1400
Indianapolis, IN 46204
Telephone: (317) 636-6481
Facsimile: (317) 636-2593
ltoops@cohenmalad.com
athomas@cohenmalad.com

**UNITED STATES DISTRICT COURT**
**DISTRICT OF ARIZONA**

| | |
|---|---|
| William Ciminski, on behalf of himself and all others similarly situated,<br><br>Plaintiff,<br><br>vs.<br><br>VectraRx Mail Pharmacy Services, LLC.<br><br>Defendant. | Case No.<br><br>**COMPLAINT—CLASS ACTION**<br><br>**DEMAND FOR JURY TRIAL** |

Plaintiff William Ciminski, (collectively, "Plaintiff"), by and through his attorneys, upon personal knowledge as to his own acts and experiences, investigation of their counsel, and upon information and belief as to all other matters, allege as follows:

## NATURE OF THE ACTION

1. Defendant VectraRx Mail Pharmacy Services, LLC ("VRMP" or "Defendant") is an Arizona prescription delivery service that provides delivery of medications for on-the-job and personal injury claims.

2. This action arises out of a recent data breach (the "Data Breach") involving

information on Defendant's network, including the personally identifiable information ("PII") of its patients, such as names, dates of birth, prescription numbers, prescription information, dates of service, and/or Social Security numbers (PHI and PII are referred to collectively as "Sensitive Information").

3. The full extent of the types of Sensitive Information, the scope of the breach, and the root cause of the Data Breach is all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation.

4. VRMP has admitted that the Sensitive Information of its patients was accessed and potentially copied by cybercriminals.

5. In total, the Data Breach exposed the Sensitive Information of thousands of current and former VRMP patients and customers ("Class Members").

6. VRMP is responsible for allowing this Data Breach because of multiple acts of negligence, including but not limited to its: failure to design, implement, and maintain reasonable data security systems and safeguards; failure to exercise reasonable care in the hiring, supervision, and training of its employees and agents and vendors; failure to comply with industry-standard data security practices; and failure to comply with federal and state laws and regulations that govern data security and privacy practices and are intended to protect the type of Sensitive Information at issue in this action.

7. Despite its role in managing so much Sensitive Information, Defendant failed to take basic security measures such as encrypting its data. Moreover, Defendant failed to recognize and detect that unauthorized third parties had accessed its network and, upon information and belief, further failed to recognize that substantial amounts of data had been compromised, and more likely than not, exfiltrated and stolen. Had Defendant not committed the acts of negligence described herein, it would have discovered the Data Breach sooner – and/or prevented the invasion and theft altogether.

8. Defendant owed numerous statutory, regulatory, contractual, and common law duties to Plaintiff and the Class Members to protect and keep their Sensitive Information confidential, safe, secure, and protected from unauthorized disclosure, access, or unconsented exfiltration, including duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and The Federal Trade Commission Act, 15 U.S.C.

§ 45. ("FTCA").

9. Moreover, by obtaining, collecting, using, and deriving benefit from Plaintiff's and Class Members' Sensitive Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Sensitive Information from disclosure.

10. As patients and/or customers of Defendant, Plaintiff and Class Members were required to provide their Sensitive Information to Defendants directly or indirectly through their treating physicians or health insurance providers.

11. In acquiring and maintaining Plaintiff's and Class Members' Sensitive Information, Defendant expressly and impliedly promised to safeguard Plaintiff's and Class Members' Sensitive Information.

12. Plaintiff and Class Members reasonably relied upon Defendant to maintain the security and privacy of the Sensitive Information entrusted to it. Plaintiff and Class Members further relied on Defendant to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

13. Plaintiff and Class Members reasonably expected and understood that Defendant would ensure that it would comply with its numerous duties, promises, and obligations to keep Plaintiff's Sensitive Information secure and safe from unauthorized access.

14. Plaintiff and Class Members would not have paid the amounts they paid for pharmacy services, had they known their information would be maintained using inadequate data security systems. Defendant, however, breached its duties, promises, and obligations, and Defendant's failures increased the risk that Plaintiff's Sensitive Information would be compromised in the event of a likely cyberattack.

15. In this era of frequent data security attacks and data breaches, particularly in the healthcare industry, Defendant's failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

16. Upon information and belief, as a result of Defendant's failures to protect the Sensitive Information of Plaintiff and Class Members, their Sensitive Information was

disclosed, accessed, downloaded, and/or exfiltrated by malicious cyber criminals, who targeted that information through their wrongdoing. As a direct and proximate result, Plaintiff and the Class Members are now at a significant present and future risk of identity theft, financial fraud, health care identity fraud, and/or other identity-theft or fraud, imminently and for years to come.

17. In the months and years following the Data Breach, Plaintiff and the other Class Members will experience numerous types of harms as a result of Defendant's ineffective and inadequate data security measures. Some of these harms will likely include fraudulent charges on financial accounts, opening fraudulent financial accounts, acquiring medical procedures and prescriptions ordered in patients' names, and targeted advertising without patient consent.

18. Plaintiff and Class Members have also now lost the economic value of their Sensitive Information. Indeed, there is both a healthy black market and a legitimate market for that Sensitive Information. Just as Plaintiff's and Class Members' Sensitive Information were stolen, *inter alia*, because of its inherent value in the black market, the inherent value of Plaintiff's and the Class Members' Sensitive Information in the legitimate market is now significantly and materially decreased.

19. Plaintiff and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their Sensitive Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) the diminution in value of their personal data; (h) the loss of value of the bargain for paying for services that required entrusting their Sensitive Information to Defendant with the mutual understanding that Defendant would safeguard the Sensitive Information against improper disclosure, misuse, and theft; and (h) the continued risk to their Sensitive Information, which remains in the possession of Defendant, and which is subject to further breaches, so

long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information.

20. Plaintiff seeks to remedy these harms, and to prevent their future occurrence, on behalf of himself and all similarly situated persons whose Sensitive Information were compromised as a result of the Data Breach.

21. Accordingly, Plaintiff, on behalf of himself and other Class Members, asserts claims for negligence (Count I); breach of implied contract (Count II); violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.* (Count III); and violation of the California Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.* (Count IV). Plaintiff seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

## THE PARTIES

***Plaintiff William Ciminski***

22. Plaintiff William Ciminski is a resident and citizen of the State of California and intends to remain domiciled in and a citizen of the State of California.

23. On or around February 6, 2025, Plaintiff Ciminski received a letter from Defendant concerning the Data Breach. The letter stated that unauthorized actors accessed VRMP's network containing his name, date of birth, prescription number, prescription information, and/or date of service.

***Defendant VRMP***

24. Defendant VRMP is a limited liability company organized in the State of Arizona. It is headquartered in Oro Valley, Arizona.

## JURISDICTION & VENUE

25. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2), because this is a putative class action involving more than 100 Class Members and because the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Moreover, Plaintiff Ciminski is a citizen of the State of California and Defendant is a citizen of the State of Arizona. Accordingly, minimal diversity under CAFA exists because Defendant as an LLC is a citizen of the State of Arizona and Plaintiff Ciminski is a citizen of the State of California.

26. This Court has general personal jurisdiction over Defendant because Defendant is organized in Arizona and has its principal place of business in Oro Valley, Arizona.

## FACTUAL ALLEGATIONS

27. VRMP is a prescription delivery service in Arizona.[1] Providing home delivery of medications for on-the-job and personal injury claims, VRMP works with physicians and payors.[2] Payment for VRMP is billed and collected from users' workers compensation or an auto insurance carrier directly.[3]

28. On or about December 13, 2024, VRMP identified suspicious activity on a server operated by VRMP. VRMP later completed its review on January 7, 2025 and determined that an unauthorized party had gained access to its network. During that time, the unauthorized party accessed files containing the Sensitive Information of VRMP's patients.

29. VRMP did not begin notifying its patients that their Sensitive Information had been compromised until it began mailing notification letters, such as the one received by Plaintiff, on or about February 6, 2025.

30. The letters received by Plaintiff and Class Members indicate that the following Sensitive Information was exposed in the breach: patient names, names, dates of birth, prescription numbers, prescription information, dates of service, and/or Social Security numbers.

31. The notification letters provided to Plaintiff and Class Members recommend several time-consuming steps that victims of the Data Breach can take to try to mitigate the risk of future fraud and identity theft, such as fraud alerts and credit freezes. Even the notice letters to Class Members, such as the one received by Plaintiff Ciminski, recognize that it was "deeply disturbed by the situation" and that the incident may have caused the letter recipients to suffer "inconvenience."

32. Patients whose Sensitive Information were determined to be exposed in the

[1] https://www.vectrapharmacy.com/notice-of-data-event
[2] https://www.vectrapharmacy.com/
[3] https://www.vectrapharmacy.com/frequently-asked-questions

Data Breach, such as Plaintiff, were offered a one or two-year subscription to credit monitoring and identity protection services. VRMP has not offered to extend this credit monitoring longer for an amount of time sufficient to protect Plaintiff and Class Members from the present, imminent, and substantially increased risk of fraud and identity theft both now and for years to come.

33. But for Defendant's failure to take reasonable steps to secure Plaintiff's and Class Members' Sensitive Information and to exercise reasonable care in the hiring and/or supervision of its employees, malicious actors would not have been able to gain access to Defendant's network.

34. The Sensitive Information in the Data Breach was unencrypted and was exfiltrated by the hackers who accessed Defendant's system.

35. It is common sense that the criminal(s) that breached Defendant's systems and acquired the victims' Sensitive Information did so for the purpose of using that data to commit fraud, theft, and other crimes, or for the purpose of the selling or providing the Sensitive Information to other individuals intending to commit fraud, theft, and other crimes. Given that this is the reason such Sensitive Information are sought by criminals, it is similarly common sense that Plaintiff and the Class Members have already suffered injury and face a substantial risk for imminent and certainly impending future injury.

36. Defendant acknowledged the risk faced by victims of the Data Breach. For example, Defendant has offered to provide Plaintiff with a one or two-year membership to credit monitoring services. It is common sense that Defendant would not pay for such services if it did not believe Plaintiff and Class Members faced a substantial risk of harm from the exposure of their Sensitive Information in the Data Breach.

37. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[4] Identity thieves use stolen personal information for a variety of crimes,

[4] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited April 20, 2021). https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

including credit card fraud, phone or utilities fraud, and bank and finance fraud.[5]

38. The physical, emotional, and social toll suffered (in addition to the financial toll) by identity theft victims cannot be understated.[6] "A 2016 Identity Theft Resource Center survey of identity theft victims sheds light on the prevalence of this emotional suffering caused by identity theft: 74 percent of respondents reported feeling stressed, 69 percent reported feelings of fear related to personal financial safety, 60 percent reported anxiety, 42 percent reported fearing for the financial security of family members, and 8 percent reported feeling suicidal."[7]

39. More recently, the FTC released an updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

40. The FTC has brought enforcement actions against businesses for failing to protect customers' PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. §45.

41. Identity thieves may commit various types of crimes such as, *inter alia*, immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, fraudulently obtaining medical services, and/or using the victim's information to obtain a fraudulent tax refund.

42. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected. Moreover, identify thieves

---

[5] *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

[6] *Id.*

[7] *Id.*

may wait years before using the stolen data.

43. Because the information Defendant allowed to be compromised and taken is of such a durable and permanent quality (*i.e.*, names, Social Security Numbers, dates of birth, and PHI), the harms to Plaintiff and the Class will continue and increase, and Plaintiff and the Class will continue to be at substantial risk for further imminent and future harm.

***Defendant Knew It Was and Continues to Be a Prime Target for Cyberattacks.***

44. Defendant is fully aware of how sensitive the Sensitive Information it stores and maintains is. It is also aware of how much Sensitive Information it collects, uses, and maintains from Plaintiff and Class Members.

45. Defendant knew or should have known that it was an ideal target for hackers and those with nefarious purposes related to sensitive personal and health data. It processed and saved multiple types, and many levels, of Sensitive Information through its computer data and storage systems.

46. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiff's and the Class Members' Sensitive Information, Defendant assumed certain legal and equitable duties, and it knew or should have known that it was responsible for the diligent protection of that Sensitive Information it collected and stored.

47. As a large and highly successful company, Defendant had the resources to invest in the necessary data security and protection measures. Yet, Defendant failed to exercise reasonable care in the hiring and/or supervision of its employees and agents and failed to undertake adequate analyses and testing of its own systems, adequate personnel training, and other data security measures to avoid the failures that resulted in the Data Breach.

48. The seriousness with which Defendant should have taken its data security is shown by the number of data breaches perpetrated in the healthcare industry over the past few years.

49. Over 41 million patient records were breached in 2019, with a single hacking incident affecting close to 21 million records.[8] Healthcare breaches in 2019 almost tripled

[8] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEATLHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-

those the healthcare industry experienced in 2018, when 15 million patient records were affected by data breach incidents, according to a report from Protenus and DataBreaches.net.[9]

50. Protenus, a healthcare compliance analytics firm, analyzed data breach incidents disclosed to the U.S. Department of Health and Human Services or the media during 2019, finding that there has been an alarming increase in the number of data breaches of patient privacy since 2016, when there were 450 security incidents involving patient data.[10] In 2019 that number jumped to 572 incidents, which is likely an underestimate, as two of the incidents for which there were no data affected 500 dental practices and clinics and could affect significant volumes of patient records. There continues to be on average at least one health data breach every day.[11]

51. One recent report found that in 2020, healthcare was one of the industries most affected by tracked ransomware incidents.[12]

***PII and PHI Are Very Valuable***

52. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[13]

---

records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=Over%2041%20million%20patient%20records, close%20to%2021%20million%20records (last visited December 23, 2021).

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] Kat Jerich, *Healthcare hackers demanded an average ransom of $4.6 last year, says BakerHostetler*, HEALTHCARE IT NEWS (May 4, 2021), https://www.healthcareitnews.com/news/healthcare-hackers-demanded-average-ransom-46m-last-year-says-bakerhostetler (last visited December 23, 2021).

[13] *The Information Marketplace: Merging and Exchanging Consumer Data*, FTC (Mar. 13, 2001), *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited December 23, 2021).

53. Consumers rightfully place a high value not only on their PII and PHI, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[14] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the internet is in everyday lives since then indicates that these values—when associated with the loss of Sensitive Information to bad actors—would be exponentially higher today.

***The PII and PHI at Issue Here is Particularly Valuable to Hackers***

54. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers, but credit and debit cards can be cancelled, quickly mitigating the hackers' ability to cause further harm. Instead, PHI and types of PII that cannot be easily changed (such as dates of birth and Social Security Numbers) are the most valuable to hackers.[15]

55. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

56. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor

---

[14] Il-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited December 23, 2021).

[15] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters., https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited December 23, 2021).

> vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[16]

57. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[17] Victims of the Data Breach will spend, and already have spent, time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

58. PHI is just as, if not more, valuable than Social Security Numbers. According to a report by the Federal Bureau of Investigation's ("FBI") Cyber Division, healthcare records can be sold by criminals for 50 times the price of stolen Social Security numbers or credit card numbers.[18] A file containing private health insurance information can be bought for between $1,200 and $1,300 ***each*** on the black market.[19]

---

[16] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited December 23, 2021).

[17] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

[18] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (last visited December 23, 2021).

[19] Elizabeth Clarke, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents*, SecureWorks (July 15, 2013),

59. Similarly, the most recent edition of the annual Baker Hostetler Data Security Incident Response Report found that in 2020, hackers in ransomware attacks made an average initial ransomware demand of $4,583,090 after obtaining PHI. In 2020, final payouts to hackers committing ransomware attacks involving PHI averaged $910,335.[20]

60. Companies recognize that Sensitive Information are valuable assets. Indeed, Sensitive Information are valuable commodities. A "cyber black-market" exists in which criminals openly post stolen Sensitive Information on a number of Internet websites. Plaintiff's and Class Members' compromised Sensitive Information has a high value on both legitimate and black markets.

61. Some companies recognize PII, and especially PHI, as a close equivalent to personal property. Software has been created by companies to value a person's identity on the black market. The commoditization of this information is thus felt by consumers as theft of personal property in addition to an invasion of privacy.

62. Moreover, compromised health information can lead to falsified information in medical records and fraud that can persist for years as it "is also more difficult to detect, taking twice as long as normal identity theft."[21]

63. Because the information Defendant allowed to be compromised and taken is of such a durable and permanent quality, the harms to Plaintiff and the Class will continue and increase, and Plaintiff and Class Members will continue to be at substantial risk for further imminent and future harm.

***Defendant's Post-Breach Activity Was (and Remains) Inadequate***

64. The information stolen allows criminals to commit theft, identity theft, and other types of fraud. Moreover, because the data points stolen are persistent—for example, names, dates of birth, Social Security numbers, and prescription medication data—as opposed to transitory, criminals who access, stole, or purchase the Sensitive Information belonging to Plaintiff and the Class Members, do not need to use the information to commit

---

https://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents (last visited December 23, 2021).

[20] Jerich, *supra* n.12.

[21] *See* FBI, *supra* n.18.

fraud immediately. The Sensitive Information can be used or sold for use years later, and often is.

65. Plaintiff and Class Members are now at a significant risk of imminent and future fraud, misuse of their Sensitive Information, and identity theft for many years in the future as a result of the Defendant's actions and the Data Breach. The theft of their PHI is particularly impactful, as many banks or credit card providers have substantial fraud detection systems with quick freeze or cancellation programs in place, whereas the breadth and usability of PHI allows criminals to get away with misuse for years before healthcare-related fraud is spotted.

66. Plaintiff and Class Members have suffered real and tangible losses, including but not limited to the loss in the inherent value of their Sensitive Information, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries.

67. Despite Defendant's egregious failure to protect Plaintiff's Sensitive Information, it has only offered to provide them with trivial compensation or remedy, such as one or two years of credit monitoring or identity protection services.

## PLAINTIFF'S EXPERIENCE

***Plaintiff William Ciminski***

68. Ciminski believes he used VRMP's services when he had an eyeglass prescription filled through his doctor's office. To receive services at VRMP, Plaintiff Ciminski was required to provide his Sensitive Information directly to Defendant, which, upon information and belief, was provided by his treating physician, or health insurance, and was then entered into VRMP's database and maintained by Defendant.

69. Plaintiff provided his Sensitive Information to VRMP and trusted that the company would use reasonable measures to protect it according to VRMP's internal policies and state and federal law.

70. Plaintiff Ciminski is very careful about sharing his Sensitive Information. Plaintiff stores any documents containing his Sensitive Information in a safe and secure location. He has never knowingly transmitted unencrypted Sensitive Information over the internet or any other unsecured source.

71. At the time of the Data Breach—December 13, 2024—Defendant retained Plaintiff's Sensitive Information in its system, despite no longer maintaining a relationship with Plaintiff.

72. Plaintiff Ciminski received the Notice Letter, by U.S. mail, directly from Defendant, dated February 6, 2025. According to the Notice Letter, Plaintiff's Sensitive Information was improperly accessed and obtained by unauthorized third parties, including his full name, date of birth, prescription number, prescription information, and/ or dates of service. Plaintiff has spent significant time remedying the breach—time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

73. Upon receiving the Notice Letter from Defendant, Plaintiff Ciminski has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, signing up for the credit monitoring and identity theft insurance offered by Defendant, and contacting financial institutions to ensure his accounts are secure.

74. Subsequent to the Data Breach, Plaintiff Ciminski has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of Sensitive Information; (iii) lost or diminished value of Sensitive Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his Sensitive Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information.

75. Plaintiff Ciminski additionally suffered actual injury and damages as a result of the Data Breach. Implied in his agreement as a patient of VRMP was the requirement that it adequately safeguard his Sensitive Information and that it would delete or destroy his

Sensitive Information after Defendants were no longer required to retain it. Plaintiff Ciminski would not have used VRMP had Defendant disclosed that it lacked data security practices adequate to safeguard Sensitive Information.

76. Plaintiff Ciminski further suffered actual injury in the form of damages and diminution in the value of his Sensitive Information —a form of intangible property that he entrusted to Defendant

77. Plaintiff Ciminski also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number, being in the hands of criminals.

78. Plaintiff Ciminski has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

79. Plaintiff Ciminski has a continuing interest in ensuring that his Sensitive Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

## CLASS ACTION ALLEGATIONS

80. Pursuant to the provisions of Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiff seeks to bring this class action on behalf of himself and the following nationwide class ("Nationwide Class") and California subclass ("California Subclass") (collectively, "Class") defined as:

> **Nationwide Class:** All persons who reside in the United States who received or were otherwise sent notice that their data was potentially compromised due to the Data Breach.
>
> **California Subclass:** All persons who reside in California received or were otherwise sent notice that their data was potentially compromised due to the Data Breach.

81. Excluded from the Class are Defendant; officers and directors of Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs,

predecessors, successors, and assigns of Defendant. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

82. Plaintiff reserves the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

83. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

84. All Class Members are readily ascertainable in that Defendant has access to addresses and other contact information for all Class Members, which can be used for providing notice to Class Members.

85. ***Numerosity***. The Class is so numerous that joinder of all members is impracticable. Upon information and belief, the Class contains thousands of individuals whose personal data was compromised by the Data Breach.

86. ***Commonality and Predominance***. There are numerous questions of law and fact common to Plaintiff and the Class that predominate over any questions that may affect only individual Class Members, including the following:

- whether Defendant engaged in the wrongful conduct alleged in this Complaint;
- whether Defendant's conduct was unlawful;
- whether Defendant failed to implement and maintain reasonable systems and security procedures and practices to protect customers' personal data;
- whether Defendant failed to exercise reasonable care in the hiring of its employees and agents;
- whether Defendant failed to exercise reasonable care in the supervision of its employees and agents;
- whether Defendant unreasonably delayed in notifying affected customers of the Data Breach;
- whether Defendant owed a duty to Plaintiff and Class Members to adequately

protect their personal data and to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

- whether Defendant breached its duties to protect the personal data of Plaintiff and Class Members by failing to provide adequate data security and failing to provide timely and adequate notice of the Data Breach to Plaintiff and the Class;
- whether Defendant's conduct was negligent;
- whether Defendant knew or should have known that its computer systems were vulnerable to attack;
- whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach of its systems, resulting in the loss of Class Members' personal data;
- whether Defendant wrongfully or unlawfully failed to inform Plaintiff and Class Members that it did not maintain computers and security practices adequate to reasonably safeguard customers' personal data;
- whether Defendant should have notified the public, Plaintiff, and Class Members immediately after it learned of the Data Breach;
- whether Plaintiff and Class Members suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);
- whether Plaintiff and Class Members are entitled to recover damages;
- whether Defendant's failure to implement and maintain reasonable security procedures and practices constitutes violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56;
- whether the California subclass is entitled to actual pecuniary damages under the private rights of action in the California Customer Records Act, Cal. Civ. Code § 1798.84 and statutory damages under the California Confidentiality of Medical Information Act, Civ. Code § 56, and the proper measure of such damages and/or statutory damages; and
- whether Plaintiff and Class Members are entitled to declaratory relief and

equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

87. ***Typicality***. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class Members, had their personal data compromised, breached, and stolen in the Data Breach. Plaintiff and all Class Members were injured through the uniform misconduct of Defendant, described in this Complaint, and assert the same claims for relief.

88. ***Adequacy***. Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff retained counsel who are experienced in Class action and complex litigation. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other Class Members.

89. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by

the Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

90. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

91. Particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

(a) Whether Plaintiff's and Class Members' Sensitive Information were accessed, compromised, or stolen in the Data Breach;

(b) Whether (and when) Defendant knew about the Data Breach before it notified Plaintiff and Class Members and whether Defendant failed to timely notify Plaintiff and Class Members of the Data Breach;

(c) Whether Defendant owed a legal duty to Plaintiff and the Class;

(d) Whether Defendant failed to take reasonable steps to safeguard the Sensitive Information of Plaintiff and Class Members;

(e) Whether Defendant failed to adequately monitor its data security systems;

(f) Whether Defendant failed to comply with its applicable laws, regulations, and industry standards relating to data security;

(g) Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class members' PII or PHI secure;

(h) Whether Defendant's adherence to HIPAA regulations, FTC data security obligations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach

(i) Whether Defendant's failure to implement and maintain reasonable security procedures and practices constitutes violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56; and

(j) Whether the California subclass is entitled to actual pecuniary damages under the private rights of action in the California Customer Records Act, Cal. Civ. Code § 1798.84 and statutory damages under the California Confidentiality of Medical Information Act, Civ. Code § 56, and the proper measure of such damages and/or statutory damages.

92. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendant, through its uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Defendant continues to maintain its inadequate security practices, retains possession of Plaintiff's and Class Members' Sensitive Information, and has not been forced to change its practices or to relinquish Sensitive Information by nature of other civil suits or government enforcement actions, thus making injunctive and declaratory relief a live issue and appropriate to the Class as a whole.

## COUNT I
**Negligence**
**(On behalf of Plaintiff and the Class)**

93. Plaintiff incorporates paragraphs 1-92 of the Complaint as if fully set forth herein.

94. Plaintiff and Class Members were required to submit non-public Sensitive Information to Defendant in order to obtain prescription medication services.

95. By collecting, storing, and using Plaintiff's and Class Members' Sensitive Information, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the Sensitive Information it received from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

96. Defendant was required to prevent foreseeable harm to Plaintiff and Class Members, and therefore had a duty to take reasonable steps to safeguard their Sensitive

Information from unauthorized release or theft. More specifically, this duty included: (1) exercising reasonable care in the hiring, training, and/or supervision of its employees and agents entrusted with access to Plaintiff's and Class Members' Sensitive Information; (2) designing, maintaining, and testing Defendant's data security systems and data storage architecture to ensure Plaintiff's and Class Members' Sensitive Information were adequately secured and protected; (3) implementing processes that would detect an unauthorized breach of Defendant's security systems and data storage architecture in timely and adequate manner; (4) timely acting on all warnings and alerts, including public information, regarding Defendant's security vulnerabilities and potential compromise of the Sensitive Information of Plaintiff and Class Members; (5) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements; and (6) timely and adequately informing Plaintiff and Class Members if and when a data breach occurred to prevent foreseeable harm to them, notwithstanding undertaking (1)-(5) above.

97. Defendant had a common law duty to prevent foreseeable harm to Plaintiff and Class Members. The duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate hiring, training, supervision, and security practices of Defendant in its affirmative collection of Sensitive Information from Plaintiff and Class Members. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their Sensitive Information because hackers routinely attempt to steal such information for use in nefarious purposes, Defendant knew that it was more likely than not Plaintiff and Class Members would be harmed as a result.

98. Defendant's duties to use reasonable security measures also arose as a result of the special relationship that existed between it, on the one hand, and Plaintiff and Class Members, on the other hand. This special relationship, recognized in laws and regulations, arose because Plaintiff and Class Members entrusted Defendant with their Sensitive Information by virtue of receiving health benefits through Defendant. Defendant alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

99. The injuries suffered by Plaintiff and the Class Members were proximately and directly caused by Defendant's failure to exercise reasonable care in the hiring, training, and/or supervision of its employees and agents, as well as the failure to follow reasonable security standards to protect Plaintiff and the Class Members' Sensitive Information.

100. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

101. If Defendant had taken reasonable security measures and/or exercised reasonable care in the hiring, training, and supervision of its employees and agents, data thieves would not have been able to take the personal information of Plaintiff and the Class Members. The policy of preventing future harm weighs in favor of finding a special relationship between Defendant and Plaintiff and the Class. If companies are not held accountable for failing to take reasonable security measures to protect the Sensitive Information in their possession, they will not take the steps that are necessary to protect against future security breaches.

102. Defendant owed a duty to timely disclose the material fact that Defendant's computer systems and data security practices were inadequate to safeguard users' Sensitive Information from theft.

103. Defendant breached these duties through the conduct alleged in the Complaint by, including without limitation, failing to protect the Sensitive Information in its possession; failing to maintain adequate computer systems and data security practices to safeguard the Sensitive Information in its possession; allowing unauthorized access to Plaintiff's and Class Members' Sensitive Information; failing to disclose the material fact that Defendant's computer systems and data security practices were inadequate to safeguard the Sensitive Information in its possession from theft; and failing to disclose in a timely and accurate manner to Plaintiff and Class Members the material fact of the Data Breach.

104. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Sensitive Information would not have been compromised. And as a direct and proximate result of Defendant's failure to exercise

reasonable care and use commercially reasonable security measures, the Sensitive Information of Plaintiff and the Class Members were accessed by ill-intentioned criminals who could and will use the information to commit identity or financial fraud. Plaintiff and Class Members face the imminent, certainly impending and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

105. It was foreseeable that Defendant's failure to exercise reasonable care in the hiring, training, and supervision of its employees and agents and to safeguard the Sensitive Information in its possession or control would lead to one or more types of injury to Plaintiff and Class Members. And the Data Breach was foreseeable given the known, high frequency of cyberattacks and data breaches in the healthcare industry.

106. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered, and continue to suffer, damages arising from the breach as described herein and are entitled to compensatory, consequential, and nominal damages in an amount to be proven at trial.

107. Such injuries include those described above, including: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of value of the compromised Sensitive Information; illegal sale of the compromised Sensitive Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach, reviewing bank statements, payment card, statements, insurance statements, and credit reports; expenses and time spent initiating fraud alerts, decreased credit scores and ratings; lost time; other economic harm; and emotional distress.

## COUNT II
## Breach of Implied Contract
## (On Behalf of Plaintiff and the Class)

108. Plaintiff incorporates paragraphs 1-92 of this Complaint as is fully restated herein.

109. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of healthcare services, as well as implied contracts for the

Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Sensitive Information.

110. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when she first entered into the testing services agreement with Defendant.

111. The valid and enforceable implied contract Class Members entered into with Defendant include Defendant's promise to protect nonpublic Sensitive Information given to Defendant or that Defendant creates on its own from disclosure.

112. When Plaintiff and Class Members provided their Sensitive Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

113. Defendant solicited and invited Class Members to provide their Sensitive Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Sensitive Information to Defendant.

114. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

115. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

116. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide pharmacy services to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' Sensitive Information provided to obtain such benefits of such services. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Sensitive Information.

117. Both the provision of testing services and the protection of Plaintiff's and Class Members' Sensitive Information were material aspects of these implied contracts.

118. The implied contracts for the provision of pharmacy services—contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Sensitive Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter.

119. Defendant's express representations, including, but not limited to the express representations found in its privacy notices, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff and protect the privacy of Plaintiff's and Class Members' Sensitive Information.

120. Consumers of pharmacy services value their privacy, the privacy of their dependents, and the ability to keep their Sensitive Information associated with obtaining such services. Plaintiff and Class Members would not have entrusted their Sensitive Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Sensitive Information would be safeguarded and protected, or entrusted their Sensitive Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

121. A meeting of the minds occurred, as Plaintiff and Class Members agreed and provided their Sensitive Information to Defendant and/or its affiliated healthcare providers, and paid for the provided testing services in exchange for, amongst other things, both the provision of healthcare and the protection of their Sensitive Information.

122. Plaintiff and Class Members performed their obligations under the contract when they paid for Defendant's services and provided their Sensitive Information.

123. Defendant materially breached its contractual obligation to protect the nonpublic Sensitive Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

124. Defendant materially breached the terms of the implied contracts. Defendant did not maintain the privacy of Plaintiff's and Class Members Sensitive Information as evidenced by its notifications of the Data Breach to Plaintiff and Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and Class Members Sensitive Information as set forth above.

125. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

126. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

127. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated providers.

128. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Sensitive Information, the loss of control of their Sensitive Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

129. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

130. As a direct and proximate result of Defendant's breach of contract, Plaintiff are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

## COUNT III
**Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.***
**(On Behalf of Plaintiff and the California Subclass)**

131. Plaintiff incorporates paragraphs 1-92 of the Complaint as if fully set forth herein.

132. In Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information

regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

133. Defendant is a "contractor" within the meaning of Civil Code § 56.05(d) within the meaning of Civil Code § 56.06 and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Defendant, within the meaning of Civil Code § 56.05(k).

134. Plaintiffs and California subclass members are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiffs and California subclass members fear that disclosure of their medical information could subject them to harassment or abuse.

135. Plaintiffs and California subclass members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network at the time of the unauthorized disclosure.

136. Defendant, through inadequate security, allowed unauthorized third-party access to Plaintiffs' and California subclass members' medical information, without the prior written authorization of Plaintiffs and California subclass members, as required by Civil Code § 56.10 of the CMIA.

137. Defendant violated Civil Code § 56.101 of the CMIA through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the California subclass members. Defendant's conduct with respect to the disclosure of confidential PII and PHI was willful and knowing because Defendant designed and implemented the computer network and security practices that gave rise to the unlawful disclosure.

138. In violation of Civil Code § 56.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and class members' medical information in a manner that failed to preserve and breached the confidentiality of the information contained therein. Plaintiffs' and California subclass member' medical information

was viewed by unauthorized individuals including but not limited to, the hackers, individuals who purchased the Private Information on the dark web, and others, as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a). In violation of Civil Code § 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and California subclass members' medical information. Plaintiffs' and California subclass members' medical information was viewed by unauthorized individuals, as described above, as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

139. Plaintiffs' and California subclass members' medical information that was the subject of the unauthorized disclosure included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

140. In violation of Civil Code § 56.101(b)(1)(A), Defendant's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiffs' and California subclass members' medical information was viewed by unauthorized individuals including but not limited to, the hackers, individuals who purchased the Private Information on the dark web, and others, as a direct and proximate result of Defendant's violation of Civil Code § 56.101(b)(1)(A).

141. Defendant violated Civil Code § 56.36 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the California subclass members.

142. As a result of Defendant's above-described conduct, Plaintiffs and California subclass members have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36. 385. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the unauthorized disclosure, and violation of the CMIA, Plaintiffs and California subclass members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud-risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of

privacy, (iii) breach of the confidentiality of their PII and PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII and PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

143. Plaintiff, individually and for each member of the Class, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiffs and each California subclass member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

**COUNT IV**
**Violation of the California Customer Records Act,**
**Cal. Civ. Code §§ 1798.80 *et seq.*,**
**(By Plaintiff and the California Subclass)**

144. Plaintiff incorporates paragraphs 1-92 of the Complaint as if fully set forth herein.

145. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

146. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

147. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

148. Plaintiff and members of the California subclass are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant, directly and/or indirectly, for the purpose of obtaining a

service from Defendant.

149. The personal information of Plaintiff and the California subclass at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

150. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California subclass's personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California subclass. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the California subclass from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and the California subclass's nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

151. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information

of Plaintiff and the California subclass included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the California subclass by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

152. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and the California subclass were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the subclass's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

153. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

154. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;
b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
c. If the information is possible to determine at the time the notice is provided, then any of the following:
    i. the date of the breach,
    ii. the estimated date of the breach, or
    iii. the date range within which the breach occurred. The notification shall also include the date of the notice;
d. Whether notification was delayed as a result of a law enforcement

investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

155. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the California subclass. Defendant did not provide timely written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all class members. Because not all members of the class were notified of the breach in a timely manner, members could have taken action to protect their personal information, but were unable to do so because they were not timely notified of the breach.

156. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and class members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

157. As a direct consequence of the actions as identified above, Plaintiff and class members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated

with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Sensitive Information of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Sensitive Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Sensitive Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security

auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats

that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

**JURY TRIAL DEMANDED**

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Respectfully submitted,

**O'STEEN MACLEOD COMBS PLC**

Lincoln Combs
300 W. Clarendon Ave., Suite 400
Phoenix, Arizona 85013-3424
Attorneys for Plaintiff

Lynn A. Toops (*pro hac vice* forthcoming)
Amina A. Thomas (*pro hac vice* forthcoming)
**COHENMALAD, LLP**
One Indiana Square, Suite 1400
Indianapolis, IN 46204
*Counsel for Plaintiff and the Class*